European Union cyber security as an emerging research and policy field

Helena Carrapico[1] and Andre Barrinha[2]

The aim of this special section is to draw the readers' attention to what is an emerging policy field, to call for further research to be conducted on its multiple dimensions, and to encourage the expansion of the existing body of literature. Although cyber security has now become part of our daily lives and concerns, European Studies as a discipline is yet to fully embrace the area as a subject of in-depth research. The four articles in this special section are intended to contribute to filling this gap, by interrogating what kind of actor the EU is in cyber security and what forms of governance it employs in this area.

Keywords: European union; Cyber security; emerging policy; informal governance.

Although the European Union (EU) has long developed activities related to computer security and electronic communications (European Commission, 1993; Council of the European Union, 1997), it was only in the last decade that it took the conscious decision to develop a fully-fledged approach to cyber security. Faced with increasing numbers of cyber-attacks on individuals, companies and critical infrastructures, the EU discourse slowly started to reflect the idea that societal reliance on technology constituted a rapidly growing security risk that had to be adequately addressed (European Commission, 2001). This shift in discourse resulted in the EU's attempt to adopt a cooperation support role for the area of cyber security. Given that cyberspace and cyber criminals are not limited by national boundaries, the EU presented itself as the logic and efficient solution to Member States' challenge of how best to tackle cyber security threats (Council of the European Union, 2005). Such move was marked by the adoption of legal measures, such as the 2005 Council Framework Decision on Attacks against Information Systems, and the creation of new infrastructures, including the creation of the European Network and Information Security Agency (ENISA) in 2004 and of the European Cybercrime Centre at Europol (EC3), in 2013.

At the heart of this new policy area is the striving for institutional and policy coherence, which is considered to be the key to an effective response to the cyber-challenges Europe currently faces (Carrapico and Barrinha, 2017). Coherence has become particularly crucial in the EU's

[1] Helena Carrapico, Senior Lecturer, Aston University, h.farrand-carrapico@aston.ac.uk
[2] Andre Barrinha, Lecturer, University of Bath, A.Barrinha@bath.ac.uk

cyber security policy because, for a long time, its governance was highly scattered, with relevant actors working independently from each other in areas as distinct as law enforcement, critical information infrastructure protection, and defence. The continued pursuit of policy coherence, coupled with the sustained increase in attacks on critical information infrastructures and on personal and commercial data, led the EU to further reinforce its new role by publishing its first cyber security strategy in 2013 (European Commission and HREU, 2013). The strategy aimed at improving member states and the private sector's resilience to cyber threats by encouraging a higher degree of cooperation between all actors involved, greater investment in national and private sector capacities to respond to attacks, further development of cyber defence capabilities, and increased engagement with international partners (European Commission and HREU, 2013).

Since then, progress has been achieved at political, legislative and capabilities level. Where the political dimension is concerned, cybersecurity is now among one of the EU's most important priorities, with cyber security elements having been integrated transversally within other EU policies (European Commission, 2015). In terms of legislation, the EU has in recent years adopted what is its most ambitious instrument to date, the Network and Information Security (NIS) Directive, which has introduced incident reporting obligations for the private sector (including operators of essential services and digital service providers) (European Union, 2016). The reinforcement of capabilities has also been encouraged through the creation of research and innovation funding streams for cyber security (€600 million for the period 2014-2020), the further development of national infrastructures (to ensure, for instance, that every Member State has cyber security centres), and the establishment of public-private partnerships aimed at enabling the Digital Single Market (European Commission, 2017a).

In October 2017, the European Council vowed to continue to make progress on the implementation of the EU Cyber Security Strategy and on the coherence of the EU cyber security policy (European Council, 2017). This decision involves the expansion of the EU's role in this area and the streamlining of a common approach among Member States. In particular, the EU is planning to enhance ENISA's mandate, turning it into the EU's Cybersecurity Agency, and to create a cyber security certification scheme for products, services and processes to support the Digital Single Market (European Commission, 2017b). A few months earlier, in June, It had already approved a Cyber diplomacy Toolbox (Council, 2017) with the ultimate aim of reinforcing the EU's activities in this field, and potentiate a more

coordinated response in case of cyber-attacks against European targets. Despite these efforts, a number of external and internal challenges remain: externally, there continues to be a lack of public awareness of cyber security risks, a reduced capacity on the side of the private sector to respond to incidents, coupled with a limited willingness to invest more seriously in protection mechanisms, a rapid expansion of the available tools to commit cyber crime, and a continued difficulty in attribution. Internally, insufficient progress has been made in terms of countering institutional fragmentation, defining what should be understood as resilience and how it should be achieved, advancing towards binding legal norms, and appropriate levels of funding (Bendiek et Al., 2017; Stupp, 2015).

Building on this policy background, the aim of this special section is to draw the readers' attention to what is an emerging policy field, to call for further research to be conducted on its multiple dimensions, and to encourage the expansion of the existing body of literature. Although cyber security has now become part of our daily lives and concerns, European Studies as a discipline is yet to fully embrace the area as a subject of in-depth research (for recent exceptions please see Christou, 2016, and Carrapico & Barrinha, 2017). In this sense, it is lagging behind other disciplines such as Criminology, which has been exploring the issue of cyber crime for the last 20 years (Wall, 2001). Over this period, Criminology's research agenda has mainly focused on the causes, practices and impact of different forms of cyber crime, on how cyber criminals organise themselves, and on whether existing legal frameworks and law enforcement responses can efficiently counter cyber crime (Bossler, 2017). Adding the disciplinary lenses of European Studies to this field would encourage different questions, namely on the EU's understanding of cyber security, the reasons for its prioritization, and on the actors and processes that have shaped this policy.

The articles in this special section are intended to fill this gap, by interrogating what kind of actor the EU is in cyber security and what forms of governance it employs in this area. Focusing on different case studies, they reflect a EU in search of a more relevant role and a stronger mandate, but struggling to affirm itself in relation to the large international players in the field – such as the United States, Russia and China –, the private sector, and even its major Member States. Faced with a number of political, institutional, and legal challenges, it is increasingly trying to find informal governance-based solutions.

The first article, by Myriam Dunn Cavelty, introduces the readers to the concept of cyber power and its different manifestations, which it then uses to interrogate what kind of power, if any, is yield by the EU, and what that implies for its aspirations as an international actor. Among the different ways to conceptualise power, one of the most well adapted to the EU case is Klimburg's Integrated Capability Model, which identifies three distinct types of cyber power: 1) the capacity to deliver policies and instruments ('Integrated Government Capability'), 2) the ability to project norms internationally and establish partnerships with third countries ('Integrated Systems Capability'), and 3) the aptitude to convince non-State actors to support its policies ('Integrated National Capability'). Its application to the EU case indicates that the Union has different elements of cyber power in differing degrees. The author warns, however, that future aspirations of the EU as a global power will need to further reinforce its cyber dimension.

The article by Thomas Renard explores the EU's international actorness by focusing on the area of cyber diplomacy. Although the Union is not generally considered an important key player in this field, as cyberspace becomes an increasingly important dimension of the international system, the EU is adapting its strategy in the area. The article focuses particularly on the EU's efforts to integrate cyber security into its foreign policy and to engage with third country partners in this field, by asking how this process is taking place and with which instruments. In order to answer these questions, the article maps the EU's network of very diverse bilateral cyber-partnerships. The author concludes that despite the apparent limited results brought about by this form of diplomacy, the network of partnerships is fulfilling a number of roles, namely trust-building and foundation-building for future multilateral cooperation.

The article by Ben Farrand also explores the EU's cyber actorness, in this case, by concentrating on online infringements of intellectual property rights. Although this area would not traditionally fall within cyber security, the efforts to complete the Digital Single Market have led the EU to increasingly focus on the use of the Internet as an enabler of the circulation of counterfeit goods. As such, it constitutes an excellent example of how cyber security is being transversally integrated into other previously unrelated policies. Although there has been a clear political and institutional push for the incorporation of cyber security elements into this area, the move has sparked a number of legal challenges. As this case study shows, parts of EU's current legislation are inadequate to deal with online illegal activity, which has led the

European Commission to circumvent traditional legislation and propose alternative responses to counterfeiting. Through the setting up of the European Observatory on Infringements of Intellectual Property Rights, the European Commission was able to promote information exchange, facilitate coordination between the different actors in the field, share best practices and produce technical expertise, which encouraged the private sector to voluntarily comply with the norms created.

Finally, the article by George Christou looks at J-CAT, the Joint Cyber Crime Action Taskforce, which is based at Europol, in order to analyse alternative forms of EU cyber security governance. Against a background characterised by difficulties in swift and effective information sharing, lack of binding legal norms, absence of trust between actors, and challenges in prosecuting cyber criminals, more flexible instruments have emerged with the aim of bypassing formal governance structures. Within this context, the author asks what are the implications of this form of informal governance for the operational fight against cyber crime. If at a first sight the results achieved by J-CAT seem to go beyond those obtained by other EU actors dealing with cyber crime, a deeper analysis reveals, however, that despite efforts to circumvent formal governance structures, these continue to affect informal solutions, in particular in terms of asymmetry between national legislations.

Bibliography

Bendiek, A., R. Bossong, and M. Schulze (2017) 'The EU's Revised Cybersecurity Strategy- Half-Hearted Progress on Far-Reaching Challenges'. SWP Comments. 47. November.

Bossler, A. (2017) 'Cybercrime research at the crossroads: where the field currently stands and innovative strategies to move forward', in T. J. Holt (Ed.) Cybercrime through an Interdisciplinary Lens. London, New York: Routledge.

Carrapico, H. and A. Barrinha (2017) 'The EU as Coherent (cyber) security Actor?' Journal of Common Market Studies. Vol 55 (6): 1254- 1272.

Christou, G. (2016) Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy (London: Palgrave).

Council of the European Union (2017) 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")' CFSP/PESC 476, 7 June 2017.

Council of the European Union (2005) 'Council Framework Decision on Attacks against Information Systems', Official Journal of the European Union. L 69/67, 16 March.

Council of the European Union (1997) 'Action Plan to Combat Organised Crime'. Official Journal of the European Communities. No. C 251/1, 15 August.

European Commission (2017a) 'EU Cybersecurity Initiatives- Working Towards a more Secure Online Environment'. Factsheet. Available from: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf Last Accessed on 11 January 2018.

European Commission (2017b) 'Proposal for a Regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification'. COM(2017)477 final. 13 September.

European Commission (2015) 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions The European Security Agenda', COM(2015)185 final, 28 April.

European Commission (2001) 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000)890 final, 26 January.

European Commission (1993) 'Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century', COM (93) 700 final, 5 December.

European Commission and HREU (2013) 'Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the

Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN (2013) 1 final.

European Council (2017) 'European Council Conclusions'. Brussels. 19 and 20 October.

European Union (2016) 'Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union'. Official Journal of the European Union, L194/1, 19 July.

Stupp, C. (2015) EU Cybersecurity Agency lacks Funds for Research on Major Tech Issues. Euractiv. Available from : http://www.euractiv.com/section/cybersecurity/news/eu-cybersecurity-agency-lacks-funds-for-research-on-major-tech-issues/ Last Access on 11 January 2018.

Wall, D. (2001) Crime and the Internet: cybercrimes and cyberfears. London, New York: Routledge.